JACIS : Journal Automation Computer Information System Volume: **5**, Nomor **1**, **2025**, *Hal*: 45 - 56

Perancangan Aplikasi Untuk Mendeteksi Keamanan Sistem Komputer Berbasis ISO 27001

Muh Aliyazid Mude *[1], St Hajrah Masyur [2]

[*1] Universitas Muslim Indonesia Makassar; aliyazid.mude@umi.ac.id
[2] Universitas Muslim Indonesia Makassar; hajrah.mansyur@umi.ac.id

Abstrak: Keamanan komputer untuk jaringan internet penting karena tidak dapat dipisahkan dari bentuk serangan kejahatan siber yang bisa membahayakan data olehnya itu perlu berbagai upaya pengamanan dilakukan untuk mencegah terjadinya gangguan sistem keamanan IT berbasis website. Adanya kejahatan siber dapat membahayakan data penting yang tersimpan pada perangkat seperti pencurian kartu kredit, menyadap transmisi data, pemalsuan identitas, pemalsuan data, cyberstalking, penipuan, cyber spionase dan serangan siber lainnya. Karena itu perlu ada jaminan sistem keamanan aplikasi untuk memperbaiki sistem keamanan. Salah satu cara memperbaiki manajemen keamanan IT yakni mengikut standarisasi manajemen keamanan ISO 27001:2005. Pada metode ini menggunakan model yang diterapkan yakni PDAC (plan, do, act, check) 4 model inilah yang akan digunakan untuk menilai sistem keamanan suatu sistem, sehingga perlu mendektesi aplikasi tersebut apakah memiliki sistem keamanan atau belum, karenanya tools untuk bisa mendeteksi suatu sistem / aplikasi sangat penting yang pada akhirnya memberikan rekomendasi arahan agar sesuai dengan standarisasi tersebut.
Keywords: Aplikasi IT; Sistem Keamanan; ISO 27001:2005

DOI: https://doi.org/10.47134/jacis
*Correspondensi: Muh Aliyazid Mude
Email: aliyazid.mude@umi.ac.id

Receive: 9 Desember 2024
Accepted: 11 Desember 2024
Published: 10 Januari 2025

Abstrak: Computer security for internet networks is important because it cannot be separated from the form of cybercrime attacks that can endanger data, therefore various security efforts need to be made to prevent the occurrence of website-based IT security system disruptions. The existence of cybercrime can endanger important data stored on the device such as credit card theft, intercepting data transmission, identity forgery, data forgery, cyberstalking, fraud, cyber espionage and other cyber attacks. Therefore, it is necessary to guarantee the application security system to improve the security system. One way to improve IT security management is to follow the ISO 27001: 2005 security management standardization. In this method using the applied model, namely PDAC (plan, do, act, check), these 4 models will be used to assess the security system of a system, so it is necessary to detect the application whether it has a security system or not, therefore tools to be able to detect a system / application are very important which ultimately provides recommendations for direction to comply with this standardization
Keywords: IT Application; Security System; ISO 27001:2005

PENDAHULUAN

Keamanan komputer saat ini sangat penting diterapkan untuk menjaga data-data yang tersimpan pada alat penyimpanan data pada komputer lainnya[1][2], apalagi saat ini

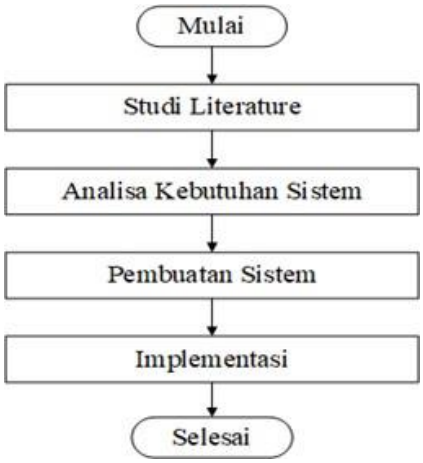
perkembangan teknologi komputer menggunakan jaringan utamanya jaringan global atau internet tidak dapat dipisahkan dari pekerjaan di berbagai bidang dalam kehidupan [3][4], pada perangkat teknologi baik pada personal komputer, handphone serta perangkat elektronika lainnya[5][6], Sehingga hal dapat berdampak pada peluang adanya kejahatan siber atau kejahatan terkait dengan jaringan internet[7]. Adapun standar sistem keamanan yang paling sering digunakan peneliti pada riset sistem keamanan komputer atau teknologi informasi adalah ISO 27001[8]. Salah satu pendekatan yang diakui secara internasional untuk manajemen keamanan informasi adalah ISO 27001:2005[9][10]. Menyediakan kerangka kerja standar untuk mengelola risiko keamanan informasi secara efektif[11]. Implementasi pada aplikasi belum diterapkan konsep dari ISO tersebut. Sehingga perlu ada pendeteksian penerapan ISO 27001:2005 pada aplikasi agar bisa diketahui seberapa besar penerapan sistem keamanan sesuai ISO tersebut. Masalah lain adalah kurangnya tools untuk mendeteksi tingkat keamanan yang diterapkan di aplikasi dimana pendeteksian sistem keamanan masih menggunakan kuesioner secara manual tanpa aplikasi.

Penelitian ini bertujuan untuk merancang aplikasi yang dapat mendeteksi tingkat keamanan sistem komputer berdasarkan ISO 27001:2005. Aplikasi ini dirancang untuk membantu mengidentifikasi penerapan ISO keamanan dalam menilai tingkat kepatuhan terhadap standarisasi. Adapun manfaat yakni mengetahui tingkat sistem keamanan yang dipakai apakah sudah sesuai standarisasi atau belum sehingga dengan rekomendasi itu diarahkan sistem yang dipakai sesuai dengan standarisasi keamanan ISO 27001:2005. Beberapa penelitan terdahulu yang terkait mengenai perancangan sistem web berbasis ISO 9126-4 dan hasilnya semua metrik dalam kondisi baik sehingga pemberikan rekomendasi untuk perbaikan IT[12], selain itu penelitian mengenai analisis manajemen keamanan informasi dengan standard iso 27001:2005 pada staff it support ternyata mampu mengurangi resiko tingkat keamanan, dan dapat melakukan evaluasi secara berkesinambungan, serta meningkatkan control keamanan yang direkomendasikan pada institusi tersebut, lain yang membahas tentang metode alternatif bagi perancangan tata kelola keamanan informasi mendapatkan hasil bahwa ISO 27001 adalah salah satu metode yang paling cocok digunakan dalam perancangan tata kelola keamanan informasi arsip digital berbasis komputasi awan [13].

Berbeda dengan beberapa hasil penelitian sebelumnya, penelitian ini difokuskan pada pengembangan aplikasi untuk mendeteksi sistem keamanan berbasis web yang mengacu pada standar ISO 27001:2005, serta dilengkapi dengan riset yang melibatkan kuesioner dan analisis jawaban responden terkait sistem keamanan tersebut.

METODE

Adapun tahapan penelitian ada 4 tahapan dimulai dengan studi literature yakni mempelajari jurnal, artikel dan berbagai informasi dari website, pada tahapan kedua menganalisa kebutuhan sistem yakni mengamati kebutuhan dan masalah yang ada dan kebutuhan untuk penyelesaian masalah sehingga diperoleh solusi masalah dengan pembuatan aplikasi deteksi keamanan, selanjutnya pembuatan sistem atau aplikasi yang didasarkan pada studi literatur pada standarisasi sistem manajemen keamanan ISO 27001:2005. Tahap selanjutnya adalah implementasi sistem yakni aplikasi diterapkan dan telah di hosting. Adapun tahapan sesuai gambar 1 berikut

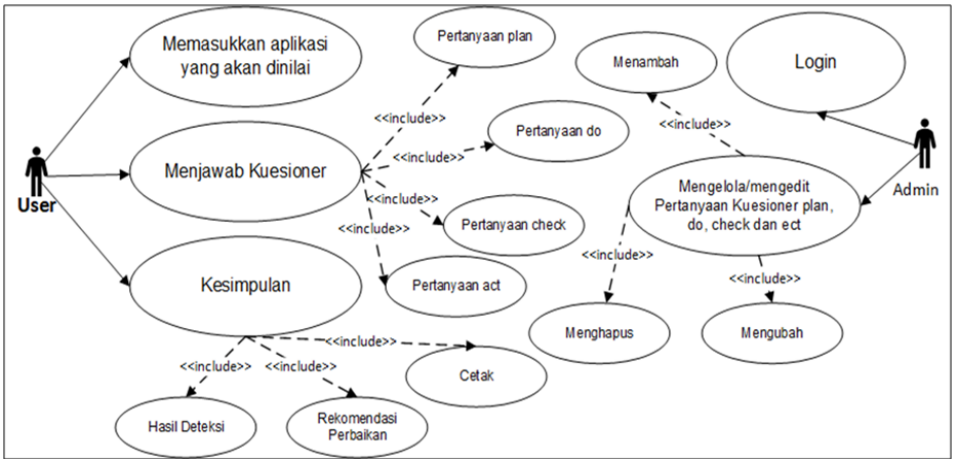


Gambar 1. Tahapan penelitian

Pada gambar 1 di studi literatur beberapa hal terkait studi pada jurnal, artikel terkait sistem keamanan, ISO keamanan 27001:2005. Khusus pada dokumen dan metode ISO 27001:2005. Berikutnya di analisa kebutuhan sistem yakni menentukan masalah yang ada, mempersiakan bahasa pemrograman yang tepat yakni php, database mysql, visual studio dan perancangan UML, serta Flowchart, penerapan PDAC ISO 27001:2005, menata kuesioner control objektifnya, selanjutnya pada pembuatan sistem yakni melakukan perancangan berdasar pada UML dan flowchart dan membuat sistem menggunakan bahasa php database mysql dengan menerapkan ISO 27001:2005. Adapun rancangan penelitian ditunjukkan pada gambar 2 berikut:

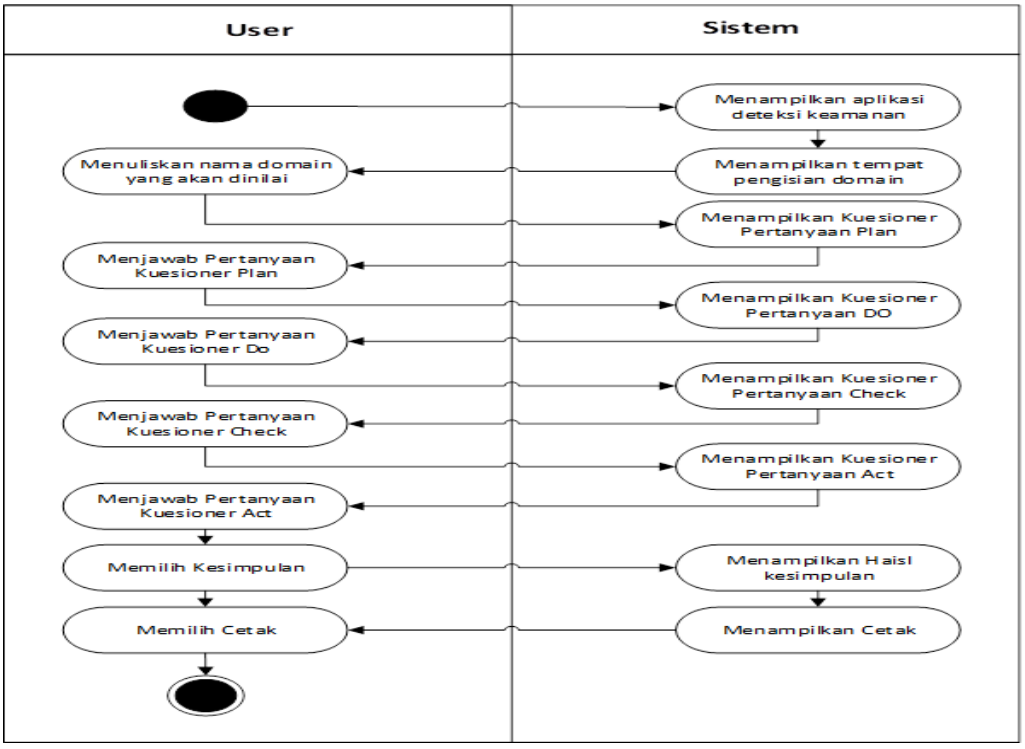
Gambar 2 Rancangan Penelitian

Gambar 2 menunjukkan pengamatan aplikasi yang diterapkan di website berbagai isu pada pemanfaatan internet oleh user dan yang paling signifikan adalah keamanan sistem, selanjutnya menyusun tahapan penelitian sesuai gambar 1, tahapan berikut adalah mengumpulkan data-data terkait keamanan sistem misal data dari jurnal, artikel, diskusi-diskusi dan menyiapkan tools lainnya, untuk tahapan berikutnya yakni merancang sistem deteksi menggunakan tools sesuai data-data yang telah dikumpulkan sebelumnya, tahapan berikut hasil berupa flatform aplikasi deteksi keamanan.



Gambar 3 *Use Case Diagram*

Rancangan sistem terlihat pada gambar 3 terdiri 2 aktor yakni user dan admin. Aktivitas yang dilakukan user yakni menginput beberapa form yang disiapkan oleh admin misal memasukkan aplikasi yang akan dinilai, menajawab kuesioner. Pada fitur kuesioner beberapa fitur sesuai PDAC Iso 27001:2005. Sementara admin memiliki beberapa otoritas pada fitur yang disiapkan termasuk perubahan kuesioner.



Gambar 4 Aktivity diagram

Aktivitas diagram gambar 4 mulai oleh user dengan menulis domain atau nama aplikasi yang akan dinilai kemudian sistem menampilkan semua model pertanyaan mulai *plan, do, check* dan act kemudian user menjawab pertanyaan yang pada akhirnya user memilih kesimpulan untuk melihat hasil yang di deteksi dan mencetak.

Populasi, sample dan sampling

Untuk populasi diambil dari beberapan riset terkait dengan sistem keamanan yang menggunakan sistem ISO 27001 utamanya ISO 27001:2005. Kemudian dari aplikasi sistem

keamanan yang ada dipilihlah 3 sampel yang berkaitan dengan metode yang digunakan dan proses penelitian utamanya pada pengambilan kuesioner untuk menentukan sistem keamanan yakni riset dengan judul perancangan sistem web berbasis iso 9126-4, analisis manajemen keamanan informasi menggunakan standard ISO 27001:2005 pada staff it support di instansi xyz dan judul ISO 27001 Sebagai metode alternatif bagi perancangan tata kelola keamanan informasi. Adapun sampling dilakukan secara acak atau simple random sampling dengan menerapkan ISO 27001:2005.

Instrumen

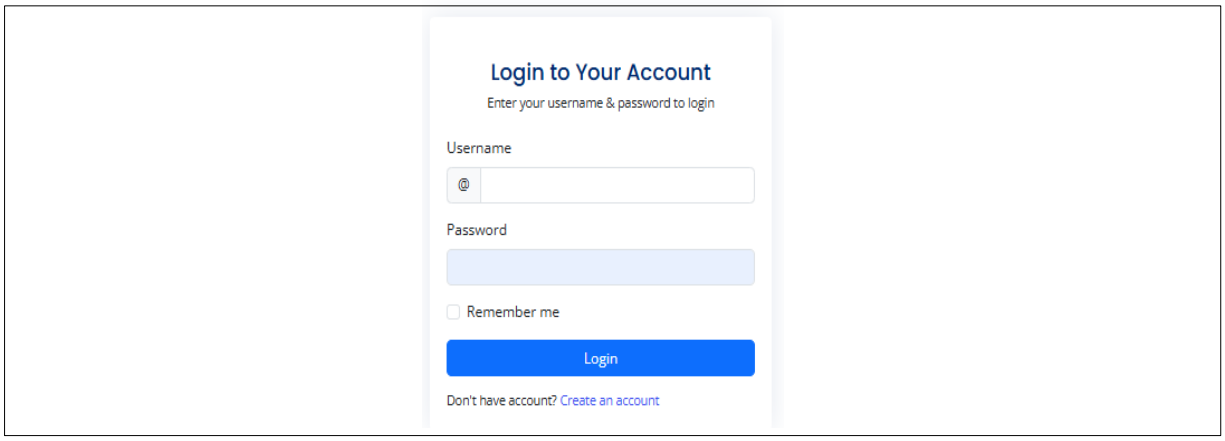
Pada bagian instrument ini terkait dengan skoring yang diterapkan merupakan modifikasi dari riset sebelumnya. Adapun peniliaan deteksi yang paling buruk atau sangat rendah adalah skor 0,00 - 0,25 dan skor paling tinggi adalah skor 0,75 – 100. Dimana setiap pertanyaan diberi nilai sesuai tingkat sensitivitas pertanyaan tersebut. Adapun pertanyaan diambil dari persepsi penulis dan kontrol objective ISO 27001:2005.

HASIL DAN PEMBAHASAN

Pada bagian tampilan awal ini terdapat bagian yakni: tampilan judul, aplikasi yang akan di deteksi keamanannya, kuesioner PDCA dan kesimpulan

Gambar 5 Tampilan Awal

Terdapat 2 bagian tugas yakni bagian (a) admin dan bagian (b) pengguna (user). Bila memilih login berarti kita sebagai admin dan beberapa fitur yang disiapkan untuk mengubah dan menambah kuesioner

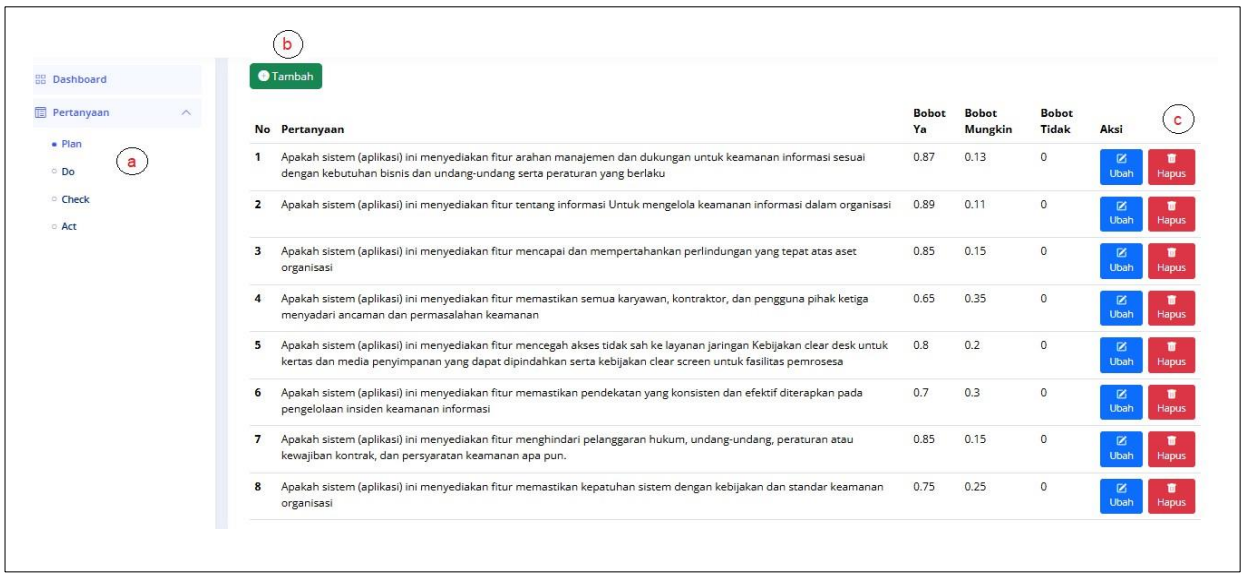


Gambar 6 tampilan awal

Memilih fitur login pada gambar 5 membawa ke login untuk admin, user name dan pasword harus diisi untuk login dan masuk pada form admin yang telah disediakan Bila login berhasil maka sistem mengantarkan kita pada dashboard admin yang bisa kita lihat pada gambar 7

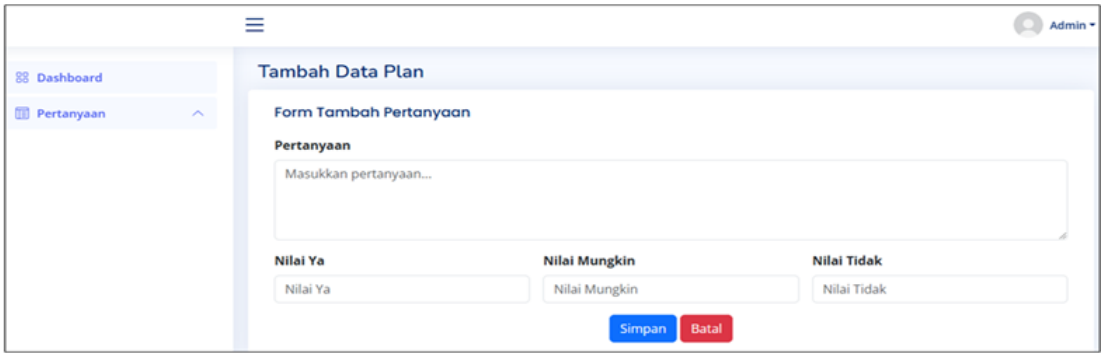
Gambar 7 Dashbord admin

Gambar 7 merupakan form admin untuk kontrol seluruh pertanyaan di kuesioner terdiri dari 4 kuesioner dan tiap kuesioner dapat diubah bentuk kuesioner. Salah satu contoh form edit pada model *plan* sesuai ilustrasi gambar 8.



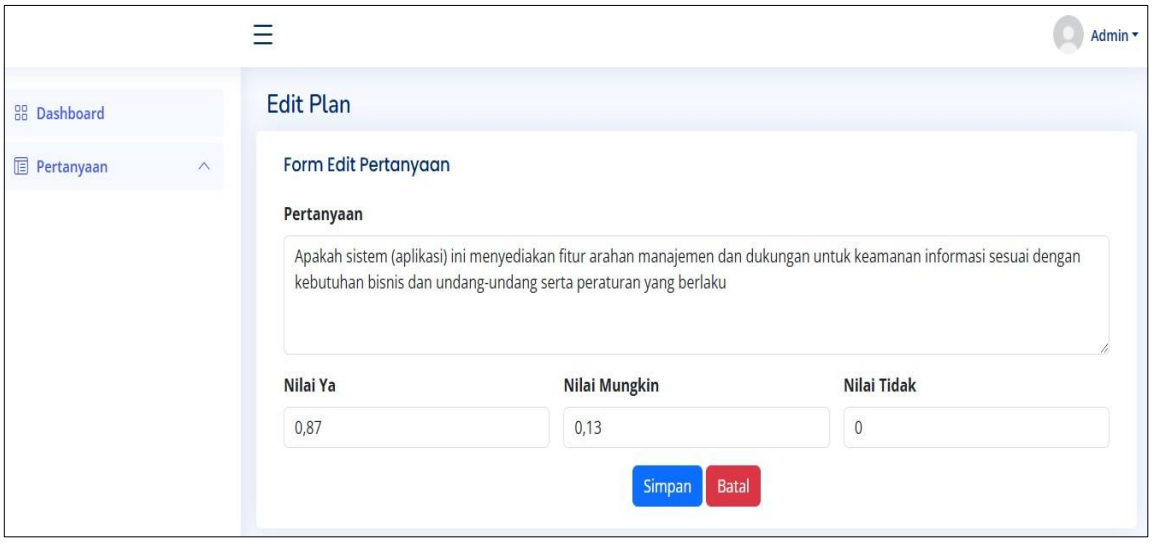
Gambar 8 Form edit

Gambar 8 menunjukkan form edit yakni: (a) form pertanyaan, (b) fitur untuk menambah pertanyaan kuesioner dan (c) mengubah dan menghapus pertanyaan. Adapun isi bagian fitur tambah (b) sesuai gambar 9.



Gambar 9 Form tambah data

Form pada gambar 9 disiapkan untuk menambah pertanyaan kuesioner berisi fitur pertanyaan bisa diinput masuk pada kolom pertanyaan setelah pemberian nilai yang terdiri nilai untuk ya, nilai mungkin, nilai tidak selanjutkan mengisi masing-masing kolom.

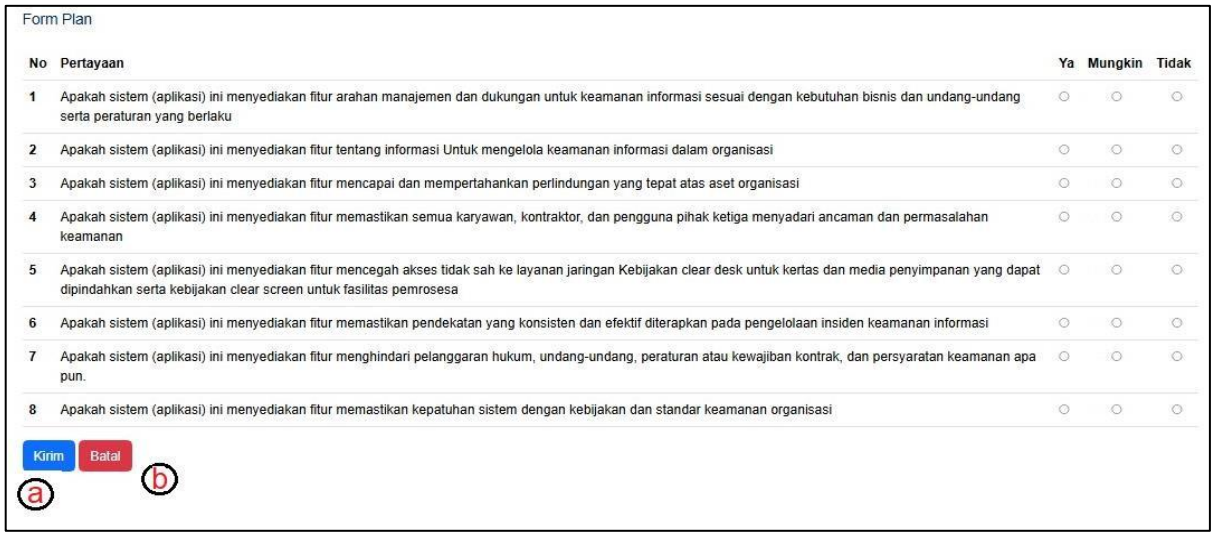


Gambar 10 Form ubah

Gambar 10 berfungsi mengubah isi pertanyaan bila ada hal tidak tepat dan form hapus bisa menghapus pertanyaan dari beberapa PDAC, sehingga tiap form pertanyaan (kuesioner) bisa dinamis sehingga tools ini bisa digunakan sesuai kebutuhan.

Gambar 11 tampilan awal aplikasi

Gambar 11 menunjukkan beberapa fungsi: untuk tampilan (a) judul yakni perancangan aplikasi untuk mendeteksi keamanan sistem komputer berbasis ISO 27001 gambar model PDCA (b). tampilan masukkan (c) bagian ini untuk memasukkan nama website yang akan dinilai dan submit untuk memulai deteksinya. Bagian (d) kuesioner yang akan dijawab sebagai dasar penilaian website. Pada bagian (e) kesimpulan terdapat fitur bisa digunakan sesuai kebutuhan. Penyusunan PDAC pada ISO 27001:2005 dengan Kuesioner plan ada 8 pertanyaan model do ada 11 pertanyaan. Model check ada 14 pertanyaan dan act 6 pertanyaan. Kesimpulan merupakan tahap akhir terdapat penilaian dan rekomendasi perbaikan tiap model. Salah satu contoh kuesioner form plan sesuai gambar 12:


Form Plan

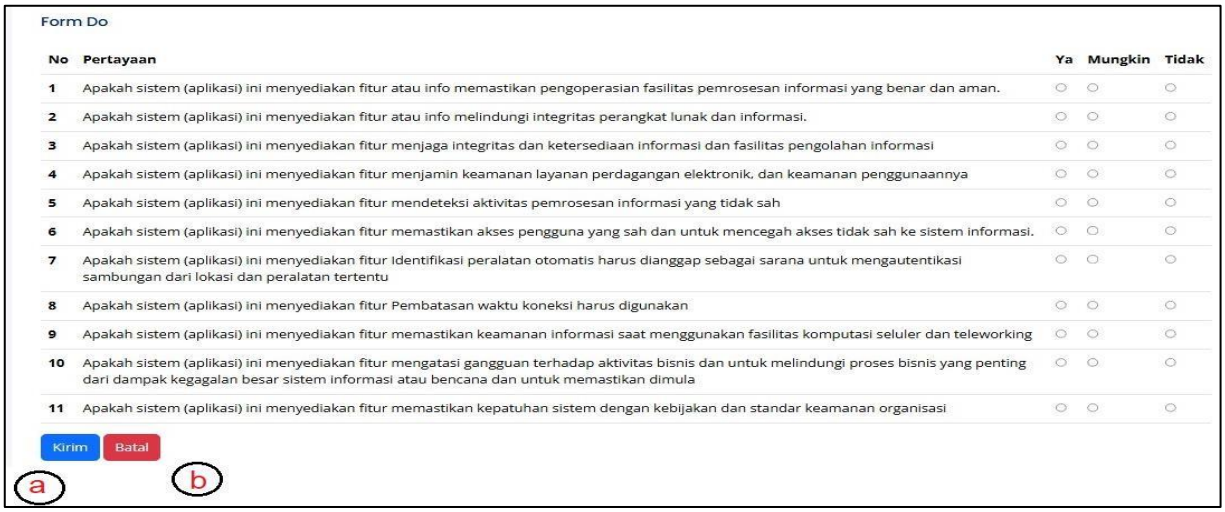
No	Pertayaan	Ya	Mungkin	Tidak
1	Apakah sistem (aplikasi) ini menyediakan fitur arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan kebutuhan bisnis dan undang-undang serta peraturan yang berlaku	○	○	○
2	Apakah sistem (aplikasi) ini menyediakan fitur tentang informasi Untuk mengelola keamanan informasi dalam organisasi	○	○	○
3	Apakah sistem (aplikasi) ini menyediakan fitur mencapai dan mempertahankan perlindungan yang tepat atas aset organisasi	○	○	○
4	Apakah sistem (aplikasi) ini menyediakan fitur memastikan semua karyawan, kontraktor, dan pengguna pihak ketiga menyadari ancaman dan permasalahan keamanan	○	○	○
5	Apakah sistem (aplikasi) ini menyediakan fitur mencegah akses tidak sah ke layanan jaringan Kebijakan clear desk untuk kertas dan media penyimpanan yang dapat dipindahkan serta kebijakan clear screen untuk fasilitas pemrosesa	○	○	○
6	Apakah sistem (aplikasi) ini menyediakan fitur memastikan pendekatan yang konsisten dan efektif diterapkan pada pengelolaan insiden keamanan informasi	○	○	○
7	Apakah sistem (aplikasi) ini menyediakan fitur menghindari pelanggaran hukum, undang-undang, peraturan atau kewajiban kontrak, dan persyaratan keamanan apa pun.	○	○	○
8	Apakah sistem (aplikasi) ini menyediakan fitur memastikan kepatuhan sistem dengan kebijakan dan standar keamanan organisasi	○	○	○

Kirim Batal

a b

Gambar 12. Form plan

Setelah mengisi seluruh pertanyaan yang diharapkan bisa menjawab pertanyaan secara berurut, namun bisa juga menjawab pertanyaan tidak berurut tapi seluruh pertanyaan harus terjawab semua agar menghasilkan kesimpulan yang diharapkan. Pilih dengan klik tombol kirim (a) untuk diproses jawabannya, dan sistem membawa ke form awal sesuai gambar 11. Adapun tombol (b) cancel membatalkan. Kuesioner do sesuai gambar 13, kuesiner chect gambar 14 dan gambar 15 adalah mode act memiliki langkah-langkah yang sama dalam menjawab pertanyaan kuesioner


Form Do

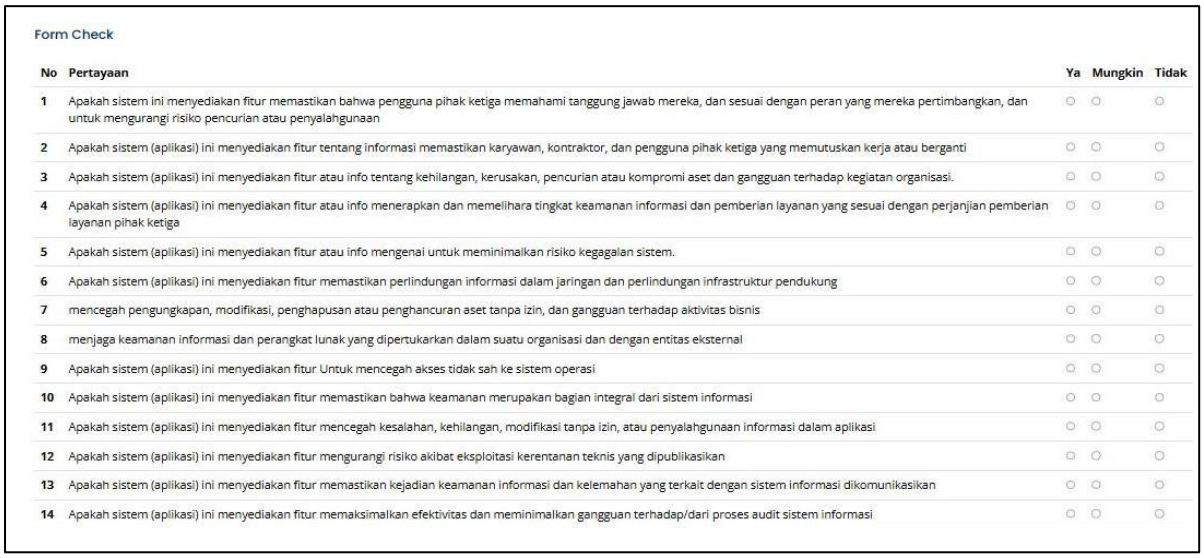
No	Pertayaan	Ya	Mungkin	Tidak
1	Apakah sistem (aplikasi) ini menyediakan fitur atau info memastikan pengoperasian fasilitas pemrosesan informasi yang benar dan aman.	○	○	○
2	Apakah sistem (aplikasi) ini menyediakan fitur atau info melindungi integritas perangkat lunak dan informasi.	○	○	○
3	Apakah sistem (aplikasi) ini menyediakan fitur menjaga integritas dan ketersediaan informasi dan fasilitas pengolahan informasi	○	○	○
4	Apakah sistem (aplikasi) ini menyediakan fitur menjamin keamanan layanan perdagangan elektronik, dan keamanan penggunaannya	○	○	○
5	Apakah sistem (aplikasi) ini menyediakan fitur mendeteksi aktivitas pemrosesan informasi yang tidak sah	○	○	○
6	Apakah sistem (aplikasi) ini menyediakan fitur memastikan akses pengguna yang sah dan untuk mencegah akses tidak sah ke sistem informasi.	○	○	○
7	Apakah sistem (aplikasi) ini menyediakan fitur Identifikasi peralatan otomatis harus dianggap sebagai sarana untuk mengautentikasi sambungan dari lokasi dan peralatan tertentu	○	○	○
8	Apakah sistem (aplikasi) ini menyediakan fitur Pembatasan waktu koneksi harus digunakan	○	○	○
9	Apakah sistem (aplikasi) ini menyediakan fitur memastikan keamanan informasi saat menggunakan fasilitas komputasi seluler dan teleworking	○	○	○
10	Apakah sistem (aplikasi) ini menyediakan fitur mengatasi gangguan terhadap aktivitas bisnis dan untuk melindungi proses bisnis yang penting dari dampak kegagalan besar sistem informasi atau bencana dan untuk memastikan dimula	○	○	○
11	Apakah sistem (aplikasi) ini menyediakan fitur memastikan kepatuhan sistem dengan kebijakan dan standar keamanan organisasi	○	○	○

Kirim Batal

a b

Gambar 13 Form do

Kuesioner atau pertanyaan pada do ada 11 pertanyaan, diharapkan bisa menjawab pertanyaan secara berurut dan bisa tidak berurut, namun diharapkan semua pertanyaan bisa seluruhnya terjawab dan bila selesai menjawab maka pilih tombol kirim untuk diproses dan sistem membawa pada form model pertanyaan.

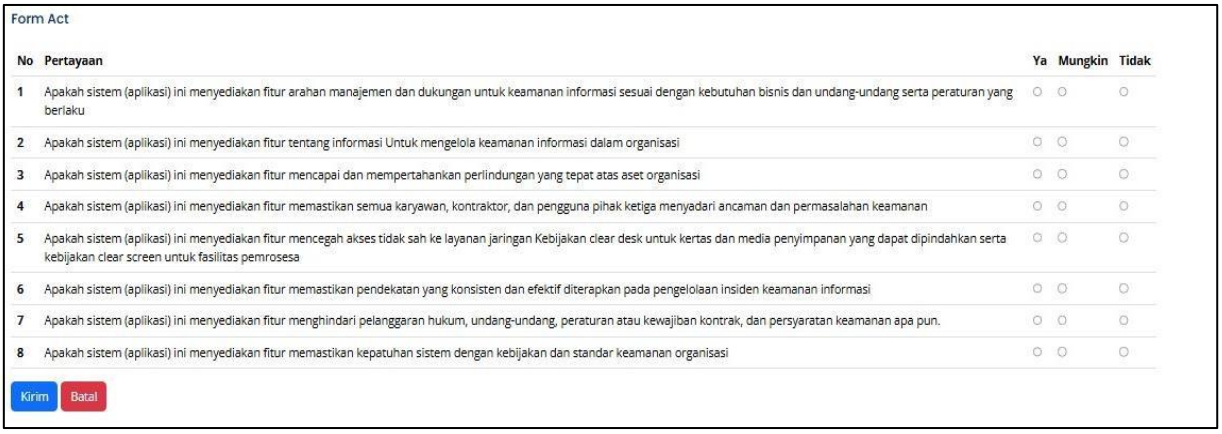


Form Check

No	Pertayaan	Ya	Mungkin	Tidak
1	Apakah sistem ini menyediakan fitur memastikan bahwa pengguna pihak ketiga memahami tanggung jawab mereka, dan sesuai dengan peran yang mereka pertimbangkan, dan untuk mengurangi risiko pencurian atau penyalahgunaan	○	○	○
2	Apakah sistem (aplikasi) ini menyediakan fitur tentang informasi memastikan karyawan, kontraktor, dan pengguna pihak ketiga yang memutuskan kerja atau berganti	○	○	○
3	Apakah sistem (aplikasi) ini menyediakan fitur atau info tentang kehilangan, kerusakan, pencurian atau kompromi aset dan gangguan terhadap kegiatan organisasi.	○	○	○
4	Apakah sistem (aplikasi) ini menyediakan fitur atau info menerapkan dan memelihara tingkat keamanan informasi dan pemberian layanan yang sesuai dengan perjanjian pemberian layanan pihak ketiga	○	○	○
5	Apakah sistem (aplikasi) ini menyediakan fitur atau info mengenai untuk meminimalkan risiko kegagalan sistem.	○	○	○
6	Apakah sistem (aplikasi) ini menyediakan fitur memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung	○	○	○
7	mencegah pengungkapan, modifikasi, penghapusan atau penghancuran aset tanpa izin, dan gangguan terhadap aktivitas bisnis	○	○	○
8	menjaga keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan entitas eksternal	○	○	○
9	Apakah sistem (aplikasi) ini menyediakan fitur Untuk mencegah akses tidak sah ke sistem operasi	○	○	○
10	Apakah sistem (aplikasi) ini menyediakan fitur memastikan bahwa keamanan merupakan bagian integral dari sistem informasi	○	○	○
11	Apakah sistem (aplikasi) ini menyediakan fitur mencegah kesalahan, kehilangan, modifikasi tanpa izin, atau penyalahgunaan informasi dalam aplikasi	○	○	○
12	Apakah sistem (aplikasi) ini menyediakan fitur mengurangi risiko akibat eksploitasi kerentanan teknis yang dipublikasikan	○	○	○
13	Apakah sistem (aplikasi) ini menyediakan fitur memastikan kejadian keamanan informasi dan kelemahan yang terkait dengan sistem informasi dikomunikasikan	○	○	○
14	Apakah sistem (aplikasi) ini menyediakan fitur memaksimalkan efektivitas dan meminimalkan gangguan terhadap/dari proses audit sistem informasi	○	○	○

Gambar 13 Form Check

Pada kuesioner check memiliki 14 pertanyaan yang diharuskan untuk dijawab agar mendapatkan hasil dan pertanyaan ini dapat ditambah dan dikurangi bila nantinya ada penyempurnaan kuesioner atau pertanyaan. Setelah menjawab semua selanjutnya memilih tombol kirim untuk menjawab pertanyaan yang ada pada modul act. Pada modul act ada 8 pertanyaan yang diharapkan bisa terjawab semua.



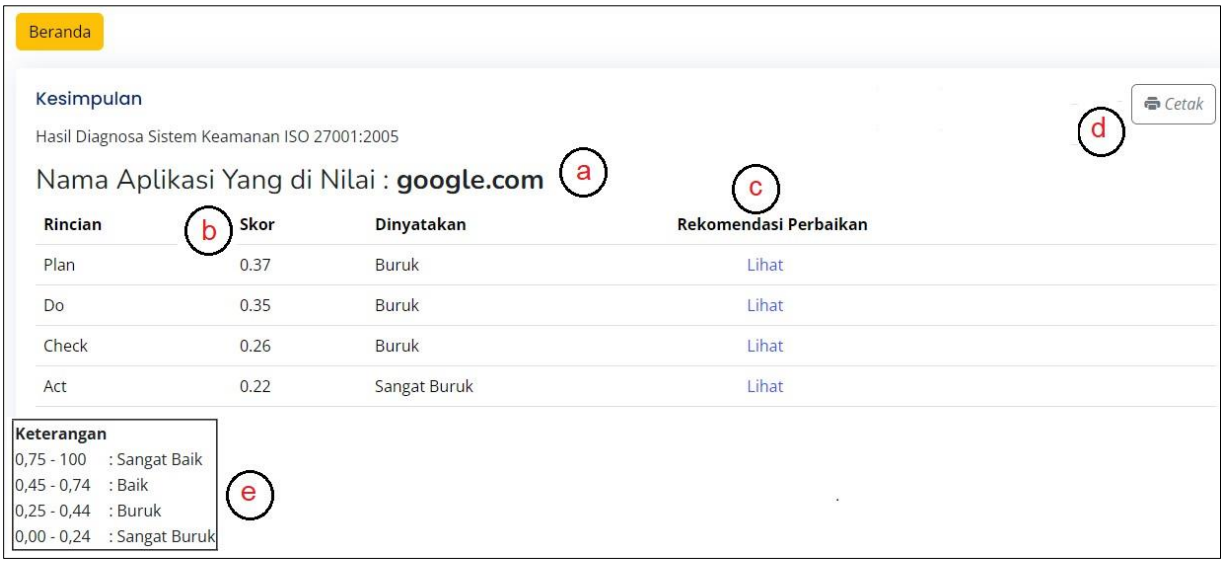
Form Act

No	Pertayaan	Ya	Mungkin	Tidak
1	Apakah sistem (aplikasi) ini menyediakan fitur arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan kebutuhan bisnis dan undang-undang serta peraturan yang berlaku	○	○	○
2	Apakah sistem (aplikasi) ini menyediakan fitur tentang informasi Untuk mengelola keamanan informasi dalam organisasi	○	○	○
3	Apakah sistem (aplikasi) ini menyediakan fitur mencapai dan mempertahankan perlindungan yang tepat atas aset organisasi	○	○	○
4	Apakah sistem (aplikasi) ini menyediakan fitur memastikan semua karyawan, kontraktor, dan pengguna pihak ketiga menyadari ancaman dan permasalahan keamanan	○	○	○
5	Apakah sistem (aplikasi) ini menyediakan fitur mencegah akses tidak sah ke layanan jaringan Kebijakan clear desk untuk kertas dan media penyimpanan yang dapat dipindahkan serta kebijakan clear screen untuk fasilitas pemrosesa	○	○	○
6	Apakah sistem (aplikasi) ini menyediakan fitur memastikan pendekatan yang konsisten dan efektif diterapkan pada pengelolaan insiden keamanan informasi	○	○	○
7	Apakah sistem (aplikasi) ini menyediakan fitur menghindari pelanggaran hukum, undang-undang, peraturan atau kewajiban kontrak, dan persyaratan keamanan apa pun.	○	○	○
8	Apakah sistem (aplikasi) ini menyediakan fitur memastikan kepatuhan sistem dengan kebijakan dan standar keamanan organisasi	○	○	○

Kirim Batal

Gambar 15 Form act

Setelah terjawab semua pertanyaan, selajutnya klik tombol kirim untuk diproses. Selanjutnya memilih kesimpulan sesuai gambar 11 huruf (e). Pada form kesimpulan terdapat fitur skor sebagai hasil akumulasi dari jawaban pada PADC dan fitur cetak dan fitur rekomendasi. Fitur rekomendasi merupakan fitur untuk mengarahkan skor yang diperoleh bisa lebih baik dari sebelumnya. Fitur rekomendasi dapat dilihat sesuai gambar 16



Gambar 16 Kesimpulan

Gambar 15 terdapat (a) nama aplikasi yang dinilai, bagian (b) ada hasil tiap model plan, do, check dan act. Bagian (c) terdapat rekomendasi yang diberikan bila pernyataan dibawah sangat baik yang hasilnya bisa di klik pada tombol lihat. Bagian (d) bisa dicetak kesimpulan yang disajikan dengan gambar 16 .dan bagian (e) ada keterangan penilaian 4 model.

Gambar 17 Cetak

kesimpulan diperoleh dari proses awal sampai akhir penilaian sistem keamanan suatu aplikasi untuk diarahkan agar sesuai dengan Iso 27001:2005

SIMPULAN

Berdasarkan hasil penelitian, tools atau sistem deteksi keamanan web berhasil dikembangkan dan diimplementasikan sesuai dengan model PDCA ISO 27001:2005, serta telah dipublikasikan pada laman *http://aplikasideteksisistemkeamanan.site*. Sementara itu, berdasarkan hasil riset kuesioner dan analisis jawaban responden terkait keamanan, diketahui bahwa sistem mampu memberikan rekomendasi perbaikan berdasarkan skor rincian yang dihasilkan dari jawaban kuesioner. Adapun saran bahwa aplikasi ini dirancang

menggunakan standar keamanan ISO 27001:2005 sementara risiko kejahatan siber selalu berubah seiring perubahan teknologi, karena itu standarisasi keamanan yang terbaru sangat utama diterapkan dengan asumsi ISO keamanan IT terbaru lebih baik dari standarisasi keamanan sebelumnya kemudian mengintegrasikan pendekatan keamanan lainnya, seperti kerangka kerja NIST, Cybersecurity Framework (CSF), CIS Controls (Center for Internet Security Controls) GDPR (General Data Protection Regulation) dan lainnya.

DAFTAR PUSTAKA

[1] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 02, no. 01, pp. 14–20, 2020.

[2] S. Farizy and E. S. Harianja, "Pengembangan Media Penyimpanan dalam Sistem Berkas (Studi Kasus Mahasiswa STMIK Eresha)," *J. Ilmu Komput. JIK*, vol. 3, no. 02, pp. 5–9, 2020.

[3] N. Nurbaiti and M. F. Alfarisyi, "Sejarah Internet di Indonesia," *JIKEM J. Ilmu Komputer, Ekon. dan Manaj.*, vol. 3, no. 2, pp. 2336–2344, 2023.

[4] A. Firdani, S. Suprapto, and A. R. Perdanakusuma, "Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 Menggunakan Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 6009–6015, 2019.

[5] F. Fredriansyah, "Model Pemanfaatan Jaringan Komputer," *J. Pendidik. Teknol. Inf.*, vol. 2, no. 1, pp. 40–43, 2023.

[6] E. Efendi, K. Yosiyana, A. Panggabean, and I. Halawa, "Teknologi Sistem Informasi Manual Dan Digital/Multimedia," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 2, pp. 11–19, 2023.

[7] M. D. Mulyawan, I. N. S. Kumara, I. B. A. Swamardika, and K. O. Saputra, "Kualitas Sistem Informasi Berdasarkan ISO/IEC 25010: Literature Review," *Maj. Ilm. Teknol. Elektro*, vol. 20, no. 1, p. 15, 2021, doi: 10.24843/mite.2021.v20i01.p02.

[8] A. Yudistira, F. Zaini, B. Sugiantoro, and Y. Riwanto, "Analisis Evaluasi Keamanan Informasi Pada Badan pemerintahan Pemerintahan XYZ Analysis Information Security Evaluation On Governnment Agency XYZ Using KAMI," *CyberSecurity dan Forensik Digit.*, vol. 7, no. 2, pp. 111–118, 2024.

[9] M. Amirinnisa and R. Bisma, "Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun," *Jeisbi*, vol. 04, no. 04, pp. 47–58, 2023.

[10] B. Aurabillah, L. Aprillia Putri, N. Citra Fadhlilla, and A. Wulansari, "Implementasi Framework Iso 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 454–460, 2024, doi: 10.36040/jati.v8i1.8736.

[11] W. Sofianda, S. Habibi Ritonga, and A. Buyung Nasution, "Evaluasi Manajemen Keamanan Sistem Informasi Pada Perusahaan PT.Wook Tecnology," *JurnalJurnal Sains Dan Teknol.*, vol. 3, no. 1, pp. 101–108, 2023.

[12] M. A. Mude and L. B. Ilmawan, "Perancangan Sistem Web Berbasis Iso 9126-4," *J. Inf. Syst. Manag.*, vol. 5, no. 2, pp. 214–218, 2024, doi: 10.24076/joism.2024v5i2.1420.

[13] D. Rutanaji, S. S. Kusumawardani, and W. W. Winarno, "ISO 27001 sebagai Metode Alternatif bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan untuk

Diterapkan di Arsip Nasional RI),” *Pros. Semin. Nas. ReTII ke-12 2017*, pp. 168–173, 2017.